April 2024

Secure Cislunar Communication Architecture: Cryptographic Capabilities and Protocols for Lunar Missions

Michael Hamblin
mhamblin1@collin.edu

Bilal Abu Bakr
Collin College, babubakr@collin.edu

Title

Secure Cislunar Communication Architecture: Cryptographic Capabilities and Protocols for Lunar Missions

Discipline

Cybersecurity and Cryptography

Digital Communications and Networking

Keywords

1. CISLUNAR
2. MOON
3. CRYPTOGRAPHY
4. PROTOCOL
5. QUIC
6. TOR
7. ISLL
8. LUNANET
9. DTN/BP
10. IPv6

CISLUNAR, MOON, CRYPTOGRAPHY, PROTOCOL, QUIC, TOR, ISLL, LUNANET, DTN/BP, IPv6

100-150 word narrative introduction

The burgeoning lunar economy demands a robust communication network. This project, initiated in collaboration with Dr. Bilal Abu Bakr in Spring of 2023, tackles the challenge of congestion and unreliable information exchange in cislunar space. We propose a secure architecture – a native IPv6 cislunar communication system – designed for real-time communication across diverse missions. By focusing on cryptographic protocols, network design, and innovative relay constellations, this project aims to guarantee seamless communication in the intricate and dynamic cislunar environment, paving the way for a secure and connected future on the moon.

250 Word Abstract

The surge in lunar missions intensifies concerns about congestion and communication reliability. This study proposes a secure cislunar architecture for real-time, cross-mission information exchange. We focus on cryptographic protocols and network design for a native IPv6 cislunar transit system.

Through a review of internet and space communication advancements, we emphasize the need for a secure network, exemplified by LunaNet. A robust data transit system with encryption is crucial for a common communication infrastructure. Traditional protocols face latency challenges. We advocate for user-friendly encryption methods to address confidentiality within the CIA Triad. Integrity is maintained through cryptographic message authentication codes. Availability is ensured by minimizing latency, implementing redundancy, and enabling dynamic re-routing.

We propose a Cislunar Relay Architecture with Pitcher and Catcher constellations. Pitcher satellites manage uplink connections, while Catcher satellites manage downlink. This mesh network configuration ensures uninterrupted communication. Secure alternatives to VPN tunneling technologies, like Optical/Laser Inter-Satellite Links, are explored.

This paper analyzes cryptographic and protocol requirements for a secure cislunar communication architecture. The Cislunar Relay Architecture offers a dependable solution for future lunar missions, guaranteeing communication in the complex cislunar environment.

MAS Abstract

2:10 SECURE CISLUNAR COMMUNICATION ARCHITECTURE: CRYPTOGRAPHIC CAPABILITIES AND PROTOCOLS FOR LUNAR MISSIONS

Michael Hamblin, Bilal Abu Bakr

Collin College - Frisco Preston Ridge Campus, TX

The surge in lunar missions propelled by nation-state rivalry and commercial ventures has spurred concerns regarding congestion and potential conflicts in lunar space and radio channels. This abstract delves into the imperative need for a robust cislunar communication architecture to facilitate reliable communication channels across diverse missions and partners. Developing such an architecture is crucial to addressing these challenges and ensuring confidentiality, integrity, availability, safety, and data segmentation for various tasks. This study explores the required cryptographic capabilities and protocols for establishing a native IPv6

cislunar transit and routing system, navigating the complexities of real-time communication in cislunar space.

The research initiates an extensive review of internet technologies and space-based communication advancements, emphasizing the necessity of a secure cislunar communication network, as exemplified by the proposed LunaNet project. To establish a common cross-mission communications infrastructure, a dependable data transit bus equipped with robust encryption algorithms is indispensable. The study highlights the limitations of traditional cryptographic protocols, particularly in real-time protocols, due to latency issues.

Focusing on the Confidentiality-Integrity-Availability (CIA) Triad, this abstract underscores the need for encryption to ensure confidentiality, emphasizing the simplification of cryptographic implementation for end-users. Integrity is maintained through cryptographic message authentication codes, guaranteeing the authenticity of communication across the network. Availability challenges are tackled by minimizing latency, ensuring multiple redundant paths, dynamic re-routing, and upholding network reliability.

A novel Cislunar Relay Architecture is proposed, comprising Pitcher and Catcher satellite constellations. Pitcher satellites in Earth orbit establish uplink connections between ground stations and commercial networks, utilizing a mesh network for continuous communication. Catcher satellites in lunar orbit mirror this function on the moon's side, offering downlink connections to lunar distribution satellites and ground stations. This combination ensures uninterrupted line-of-sight communication, enhancing network availability.

The study explores inter-satellite communication methods, considering the shortcomings of VPN tunneling technologies in dynamic virtual environments. Optical Inter-Satellite Links (OISL) and Inter-Satellite Laser Links (ISLLs) are suggested as alternatives, providing enhanced security and immunity to interference.

In conclusion, this Abstract presents a comprehensive analysis of the cryptographic and protocol requirements for a secure cislunar communication architecture. By tackling challenges associated with confidentiality, integrity, and availability, the proposed Cislunar Relay Architecture offers a dependable solution for future lunar missions, guaranteeing seamless communication in the intricate and dynamic Cislunar space environment.

Full Name and Collin contact information

Michael Hamblin

mhamblin1@collin.edu

+1 214 215 2937 cell

References

AlSabah, M., & Goldberg, I. (2015). Performance and Security Improvements for Tor: A Survey. IACR Cryptology EPrint Archive, 2015, 235. https://eprint.iacr.org/2015/235.pdf

Basyoni, L., Erbad, A., AlSabah, M., Fetais, N., Mohamed, A., & Guizani, M. (2021). QuicTor: Enhancing Tor for Real-Time Communication Using QUIC Transport Protocol. IEEE Access, 9, 28769–28784. https://doi.org/10.1109/access.2021.3059672

Border, J. R., Shah, B., Su, C., & Torres, R. (2020). Evaluating QUIC's Performance Against Performance Enhancing Proxy over Satellite Link. 2020 IFIP Networking Conference (Networking), 755–760. https://dblp.uni-trier.de/db/conf/networking/networking2020.html#BorderSST20

Burleigh, S., Hooke, A., Torgerson, L., Fall, K., Cerf, V. G., Durst, B., Scott, K., & Weiss, H. A. (2003). Delay-tolerant networking: an approach to interplanetary Internet. IEEE Communications Magazine, 41(6), 128–136. https://doi.org/10.1109/mcom.2003.1204759

Guri, M. (2022). ETHERLED: Sending Covert Morse Signals from Air-Gapped Devices via Network Card (NIC) LEDs. 2022 IEEE International Conference on Cyber Security and Resilience (CSR). https://doi.org/10.1109/csr54599.2022.9850284

Israel, D., Mauldin, K. D., Roberts, C. J., Mitchell, J. P., Pulkkinen, A., Cooper, L. V., Johnson, M. K., Christe, S., & Gramling, C. (2020). LunaNet: a Flexible and Extensible Lunar Exploration Communications and Navigation Infrastructure. IEEE Aerospace Conference. https://doi.org/10.1109/aero47225.2020.9172509

Lardinois, F. (2015, April 18). Google Wants To Speed Up The Web With Its QUIC Protocol. TechCrunch. Retrieved April 4, 2023, from https://techcrunch.com/2015/04/18/google-wants-to-speed-up-the-web-with-its-quic-protocol/

Motzigemba, M., Zech, H., & Biller, P. (2019). Optical Inter Satellite Links for Broadband Networks. International Conference on Recent Advances in Space Technologies. https://doi.org/10.1109/rast.2019.8767795

Rescorla, E., & Schiffman, A. (1999). The Secure HyperText Transfer Protocol. RFC. https://doi.org/10.17487/rfc2660

Shirazi, F., Simeonovski, M., Asgher, M., Backes, M., & Diaz, C. (2018). A Survey on Routing in Anonymous Communication Protocols. ACM Computing Surveys, 51(3), 1–39. https://doi.org/10.1145/3182658

Syverson, P., Goldschlag, D. M., & Reed, M. (1997). Anonymous connections and onion routing. IEEE Symposium on Security and Privacy. https://doi.org/10.1109/secpri.1997.601314

Wang, Y., Zhao, K., Li, W., Fraire, J. A., Sun, Z., & Fang, Y. (2018). Performance Evaluation of QUIC with BBR in Satellite Internet. 2018 6th IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE). https://doi.org/10.1109/wisee.2018.8637347

Yang, W., Shu, S., Cai, L., & Pan, J. (2021). MM-QUIC: Mobility-aware Multipath QUIC for Satellite Networks. 2021 17th International Conference on Mobility, Sensing and Networking (MSN). https://doi.org/10.1109/msn53354.2021.00093

Zhu, Q., Tao, H., Cao, Y., & Li, X. (2022). Laser Inter-Satellite Link Visibility and Topology Optimization for Mega Constellation. Electronics, 11(14), 2232. https://doi.org/10.3390/electronics11142232